

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Le traitement des données à caractère personnel dans le secteur d'assurances. La légalité des banques de données

Dhont, Jan

Published in:
Revue de Droit de l'U.L.B

Publication date:
2000

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Dhont, J 2000, 'Le traitement des données à caractère personnel dans le secteur d'assurances. La légalité des banques de données', *Revue de Droit de l'U.L.B*, VOL. 21, Numéro 1, p. 289-334.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

**LE TRAITEMENT DES DONNÉES
À CARACTÈRE PERSONNEL
DANS LE SECTEUR D'ASSURANCES
LA LÉGALITÉ DES BANQUES DE DONNÉES (*)**

PAR

JAN DHONT

CHERCHEUR AU CRID (FUNDP)

AVOCAT

INTRODUCTION

1. — Depuis toujours, le malheur et la malchance sont propres à la vie individuelle et sociale. Tandis qu'on estimait dans l'antiquité et au moyen âge que l'on pouvait se prévenir d'une grande partie des douleurs en respectant les préceptes de(s) Dieu(x), l'homme a cherché très tôt les moyens de s'assurer contre ces douleurs. Certes, non seulement le développement du marché et des moyens monétaires ont contribué au marché florissant des assurances, mais la vision du monde déterministe de la modernité y a également contribué. L'homme de la modernité est celui qui se perçoit lui-même comme un sujet de volonté pouvant tout maîtriser dans le monde (1). L'incertitude lui est étrange. Or, on pourrait définir un contrat d'assurance comme un contrat par lequel l'assuré transfère le risque, relativement faible, d'un dommage futur, qui lui est relativement important, à un assureur, en échange du paiement sûr de primes relativement petites (2). On constate qu'en estimant que le risque est considérable en

(*) *Je suis reconnaissant pour les sages indications de Dieter Verhaeghe, Marie-Noëlle Verhaegen et Jacques Wahle. De plus, mon gratitude est grande pour Laurence Hage et Myriam Lefrancq pour leur aide indispensable dans la rédaction de cette contribution.*

(1) BENSASAYAG, M., AKDAG, H. et SECROUN, Cl., *Peut-on penser le monde ?*, Hasard et incertitude, Ed. du Félin, 1997.

(2) BERGKAMP, L., *De vervuiler betaalt dubbel*, 1998, Insertia Antwerpen-Groningen, p. 53.

termes pécuniaires, l'assureur accepte de supporter ce risque en encaissant des primes payées par le preneur ou l'assuré.

2. — Le système d'assurance basé sur la solidarité organisée entre les assurés, ainsi que la concurrence de marché nécessitent que les assureurs puissent évaluer le risque économique qu'ils encourent. En termes Coasiens, ils sont confrontés à un « manque du marché » (market failure) c.à.d. des informations imparfaites ou d'un manque d'information tout court. Vu que les assurances privées s'inscrivent dans une logique commerciale, il est évident que l'assureur veuille estimer le risque afin d'ajuster la politique des prix des primes et la hauteur des franchises, etc. L'article 5 de la loi du 25 juin 1992 sur le contrat d'assurance terrestre (ci-après : LAT) consacre le droit de l'assureur à l'information du risque assuré (3). Ainsi, des informations à caractère personnel, parfois sensibles, seront récoltées et traitées lors la conclusion et durant la durée du contrat.

3. — On voit clairement que le traitement des informations relatives aux assurés devra être fait en garantissant la balance d'intérêts et des libertés entre les différents acteurs. En général, la finalité d'efficience et de lucre visées par les assureurs (avec légitimité) ne constitue-t-elle pas un risque pour la vie privée et les libertés fondamentales des assurés? L'assuré ne paie-t-il pas deux fois ces primes, n'y a-t-il pas une intrusion dans sa vie privée, ou plus fondamentalement : n'y a-t-il pas une violation d'autres libertés telles que celles d'obtenir un crédit, de se déplacer en voiture, d'obtenir des soins de santé, etc. (4)? Avec l'application croissante des nouvelles technolo-

(3) Article 5 : « Le preneur d'assurance a l'obligation de déclarer exactement, lors de la conclusion du contrat, toutes les circonstances connues de lui et qu'il doit raisonnablement considérer comme constituant pour l'assureur des éléments d'appréciation du risque. Toutefois, il ne doit pas déclarer à l'assureur les circonstances déjà connues de celui-ci ou que celui-ci devrait raisonnablement connaître. Les données génétiques ne peuvent pas être communiquées. S'il n'est point répondu à certaines questions écrites de l'assureur et si ce dernier a néanmoins conclu le contrat, il ne peut, hormis le cas de fraude, se prévaloir ultérieurement de cette omission ».

(4) Voy. aussi POULLET, Y. : « Fichiers d'assurances et respect des libertés », *Bull. Aaa.*, 1984, pp. 573-614.

gies, les collecte, conservation, et communication des données à caractère personnel augmenteront de manière exponentielle (5). (...)

4. — La légalité du traitement des données doit être appréciée en vertu des principes et des règles inscrites dans la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (6). Les principes constitués par cette loi figurent pour la plupart dans la Convention n° 108 du Conseil de l'Europe (7) et la directive OECD (8). Cette loi a été adaptée par la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données (9). Ce texte doit être interprété en référence à l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme. Cette nouvelle loi n'aura d'effet que par l'élaboration et l'adoption d'un arrêté royal d'exécution prévu pour octobre-novembre de cette année. Dès lors, on fondera l'analyse ci-après sur la nouvelle loi (ci-après : LVP).

5. — Dans le cadre de cet article il est impossible d'être exhaustif. Nos propos reflètent quelques problèmes qui découlent de l'application de la législation relative à la protection des données, nous paraissant importants ou épineux pour le secteur d'assurances. Ils ont pour but de mettre en avant les droits et obligations respectifs. Dans la première partie, l'utilisation des informations à finalités « internes » sera examinée,

(5) On pense par exemple à l'offre et la conclusion des contrats d'assurance via Internet. Voy. à cet égard le « CB Direct moet uit de rode cijfers geraken », *Financieel Economische Tijd* du 29 août 2000.

(6) *M.B.*, 18 mars 1993.

(7) Approuvé par la loi du 17 juin 1991 portant approbation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981, *M.B.*, 30 décembre 1993. Les principes inscrits dans la Convention sont plus spécifiquement affinés par les recommandations du Conseil de l'Europe. Ainsi, un projet de recommandation est en cours de préparation sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance (18^e réunion, Strasbourg, 19-21 janvier 1999).

(8) Council Recommendations Concerning Guidelines Governing the Protection of Privacy Transborder Flows of Personal Data, 20 *I.L.M.* 422 (1981), O.E.C.D. Doc. C (80) 58.

(9) *M.B.*, 3 février 1999.

tandis qu'on essayera ensuite, dans une deuxième partie, d'approfondir la problématique du traitement à des fins « externes ». Concernant ce dernier sujet, on s'attardera plus particulièrement sur la question concernant la légalité des mutuelles des informations (10). On fera l'analogie avec ce « phénomène » dans le secteur de consommation et se demandera si une législation spécifique s'impose.

2. — LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL POUR DES FINALITÉS « INTERNES »

6. — La conclusion d'une convention est un acte juridique qui nécessite un minimum d'échange d'informations. Dans le contexte de la conclusion d'un contrat d'assurance, le preneur d'assurance a l'obligation de déclarer toutes les circonstances qu'il doit raisonnablement considérer comme constituant pour l'assureur des éléments d'appréciation du risque. Ce principe, fondé sur le principe de la bonne foi, est (on l'a déjà mentionné) explicitement repris par l'article 5 LAT (11). Il s'agit d'une obligation de communication spontanée et complète qui devant permettre à l'assureur d'évaluer le risque et de déterminer le prix des primes, ou d'introduire des nouveaux taux basés sur des critères non utilisés auparavant (12). Les informations vont donc en premier lieu être traitées à des fins internes, c'est-à-dire dans le contexte d'administration et de la gestion de la relation avec le client.

Beaucoup de questions se posent ici : quels sont les droits subjectifs dont la personne concernée jouit lors du traitement de ses données ? Est-ce que ces informations peuvent être utili-

(10) Voy. « Verzekering mag niet zomaar polis opzeggen — Test-Aankoop vindt Datassur-bestand onwettelijk », *Financieel Economische Tijd*, 24 juni 2000.

(11) Voy. à cet égard COLLE, Ph., *Algemene Beginselen van het Belgisch Verzekeringsrecht*, Bruxelles, Bruylant, 1997, ch. IV; FAGNART, J.-L., « Dispositions communes : formation et exécution du contrat (commentaire des articles 4 à 23 de la loi du 25 juin 1992) », dans X., *La loi du 25 juin 1992 sur le contrat d'assurance terrestre*, Collection *Droit des Assurances*, Academia Louvain-la-Neuve, Bruxelles Bruylant, 1993.

(12) N.C.C., « The impact of international data protection regulations on special information — Intensive Sectors of Industry Final Report », 2 volumes, in *Data Security and Confidentiality. A joint research programme between ADI, GMD and N.C.C. sponsored by the Commission of the European Communities and National Governments*, January 1984.

sées pour d'autres finalités et dans quelle mesure ? Quels sont les obligations des assureurs en qualité du responsable du traitement lors du traitement ? ...

2.1. — Déclaration obligatoire en vue de la LVP

7. — Le candidat preneur d'assurance est souvent invité à remplir un questionnaire, par exemple dans le contexte d'une assurance-vie. La question se pose de savoir quelles sont les informations que l'assureur peut réclamer dans la phase pré-contractuelle. En tout cas, il est prévu que si le candidat n'a pas répondu à certaines questions écrites de l'assureur et si ce dernier a néanmoins conclu le contrat, il ne peut, hormis le cas de fraude, se prévaloir ultérieurement de cette omission (art. 5 § 2 LAT). Toutefois, en refusant de fournir la réponse à certaines questions irrelevantes, il risque de ne pas être couvert.

La réponse à la question posée ci-dessus peut être trouvée dans une lecture de la LVP et de la LAT.

Avant d'aller plus loin, on doit examiner si ce premier texte est, dans le cas d'espèce, applicable et il faut décrire quelques notions principales de ce texte.

8. — Le nouvel article 2 LVP prévoit que *lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée*. Cette disposition est libellée de façon beaucoup plus large que celle qui était contenue dans la « vieille » loi de 8 décembre 1992, qui visait seulement à garantir le droit au respect de sa vie privée lors de traitement des données à caractère personnel qui la concernent. Leonard et Poulet s'inquiètent que « c'est en effet l'ensemble des libertés et droits fondamentaux des personnes physiques qui peuvent être bafoués lors de traitements de données à caractère personnel » (13). Ceci est démontré par l'interdiction de la communication des informations génétiques ayant un caractère potentiellement discriminatoire (14). Cette libel

(13) POULET, Y. et LEONARD, Th., « la protection des données à caractère personnel en pleine (ré)évolution — La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 380.

(14) Voy. article 5 et 95 LAT.

lisation élargie confirme la vision selon laquelle la protection des données vaut, indépendamment d'une évaluation quant à l'intrusion effective dans la vie privée de la personne concernée (le « fiché ») (15). La loi est applicable au traitement des données à caractère personnel, même si ces données ne sont pas considérées faire partie de la « privacy » d'un individu.

9. — L'article 3 § 1 LVP stipule que celle-ci s'applique à *tout traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.*

Bien que la notion de « traitement » ait été enrichie — ce qui a son importance — et comprenne la collecte des données (16), la distinction controversielle entre « fichier » et « dossier » n'est pas supprimée (17). Le but du législateur était d'exclure les dossiers non automatisés du champ d'application de la loi. Par conséquence, la question doit être posée de savoir si les informations personnelles manuscrites tombent sous la protection de la loi. La réponse semble être nuancée, mais sera dans la plupart des cas positive.

Il ressort de l'article 3 § 1 précité que la loi s'applique à tout *traitement automatisé en tout ou en partie* (c'est nous qui italiquons). Dans la majorité des cas, les informations devront, au moins partiellement, être introduites dans un système automatisé (par exemple un fichier de gestion des clients avec référence aux contrats). Ainsi, la loi est d'application non seulement aux fichiers de référence, mais également aux données comprises dans les dossiers auxquels lesdits fichiers se réfèrent (18).

(15) Voy. à cet égard LEONARD, Th., note sous Civ. Bruxelles (prés.), 22 mars 1994, *J.T.*, p. 848.

(16) Voy. article 1^{er}, § 2 de la loi : « par 'traitement', on entend toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, l'effacement ou la destruction de données à caractère personnel ».

(17) La notion de « fichier » est définie comme suit : « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique » (article 1^{er}, § 3 LVP). Consultez également l'arrêt de la Cour de Cassation, peu éclairant en la matière : Cass., 1^{er} ch., 16 mai 1997, *J.T.*, 1997, p. 779.

(18) Voyez les rapports annuels de la Commission.

C'est uniquement dans l'hypothèse où les informations ne sont pas traitées par un moyen automatisé, quel qu'il soit, que l'on devra examiner si les données sont, selon des critères déterminés, accessibles. La loi, muette quant au niveau d'accessibilité à atteindre pour admettre la qualification de fichier, laisse une interprétation ouverte pouvant aller dans les deux sens.

10. — Dans la majorité des cas, le candidat preneur d'assurance se dirige vers une agence ou un courtier d'assurances. Est-ce que ces intermédiaires doivent être qualifiés de « responsable du traitement », destinataire de la plupart des obligations légales ?

Par responsable du traitement on entend *la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel* (19).

Une approche prudente et nuancée semble devoir être conseillée :

Les informations récoltées via l'intervention d'un intermédiaire sont en principe traitées pour des finalités et par des moyens déterminés par la compagnie d'assurance. C'est cette dernière qui rédigera les questionnaires et qui traitera les données en vue de son administration.

Toutefois, on pourrait envisager que le courtier d'assurance effectue ses propres traitements, par exemple pour sélectionner la couverture la plus adéquate à la demande du client, ou que certaines traces de données soient conservées en cas de sinistre.

En conclusion, ces deux catégories d'acteurs peuvent être qualifiées de « responsable du traitement » et devront par conséquent honorer les obligations inscrites dans la loi (20).

(19) Voy. article 1^{er}, § 4 LVP.

(20) Notons également que la définition légale n'exclut pas que la décision relative aux finalités et aux moyens du traitement puisse être conjointe. Ainsi, il est possible qu'un traitement ait plusieurs responsables. Voy. LEONARD, Th. et POULLET, Y., *l.c.*, 379 : « [...] si différents opérateurs de télécommunication centralisent des données relatives aux abonnés présentant des retards de paiement, ils seront chacun considérés comme responsable du traitement centralisé. Par contre, s'ils se groupent en une entité juridique distincte, cette dernière apparaîtra comme le responsable des divers traitements de données créés en son sein. On peut notamment penser aux centrales de crédit ou de risques particuliers en matière d'assurance (propres italiennes) ».

11. Revenons maintenant à la question relative au questionnaire présenté au client potentiel. Quelles sont les informations qui peuvent être récoltées, et sous quelles conditions est-ce que le traitement doit être réalisé?

La réponse doit être recherchée dans la lecture de l'article 4 LVP et l'article 5 LAT (21).

Il ressort de l'article 4 § 1, 1° de la première loi que les données à caractère personnel doivent être traitées loyalement et licitement. Pour être licite, un traitement de données doit respecter l'ensemble des prescrits légaux et réglementaires applicables (22) (23). Dans le cas d'espèce, la licéité doit être éva-

(21) Le traitement des données à caractère personnel étant principalement interdit sous le régime de la directive 95/46/CE, sauf s'il y a présence d'un fondement légitime. Concrètement, on devra s'interroger sur l'accomplissement des conditions prévues par l'article 5 de la loi. Il est stipulé notamment que le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas énumérés par ledit article, à savoir a) lorsque la personne concernée a indubitablement donné son consentement; b) lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée a donné son accord ou à l'exécution des mesures précontractuelles prises à la demande de celle-ci [...]. Par « consentement de la personne concernée », on entend toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement (article 1°, § 8 LVP). Il faut d'abord remarquer que ce consentement en réalité s'effrite, et ce surtout en cas de paiement des primes par des tiers (voy. à cet égard GELLMAN, R., « Protection of Medical Data », Giuffrè editore, Lavori congressuali, pp. 79-81). Toutefois, dans la majorité des cas, le traitement trouvera sa légalité sous le point (b). L'assureur ne pourra traiter des informations relatives à l'assuré ou à chaque autre bénéficiaire, sans que ces derniers ne soient eux-mêmes les preneurs d'assurance (à distinguer de l'assuré). Néanmoins, le traitement des données personnelles relatives aux bénéficiaires, non-contractants, peut être légitimé par l'article 5, f) LVP. Le traitement peut, selon ce tiret, être effectué lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi ne soient pas bafoués. Cette règle se réfère au principe de proportionnalité intrinsèque à l'évaluation de la légitimité du traitement. Même si le traitement est nécessaire au responsable, il ne pourra être poursuivi dès lors que l'opposition des intérêts en présence se résout en faveur de la personne concernée. Ceci implique que les autres principes de la loi soient cependant respectés. Plus particulièrement, seules les données nécessaires pour apprécier les risques pourront être traitées et les personnes concernées doivent en être informées de manière adéquate.

(22) On remarque que la loi relative à la protection des données constitue une législation cadre, qui englobe différents secteurs. Les principes compris dans cette législation seront par conséquent applicables dans les différents secteurs. Consultez à cet égard plus particulièrement LEONARD, Th., « Centrales de crédit et protection de la vie privée : incertitude et insécurité juridique », note sous Civ. Bruxelles (prés.), 13 septembre 1995, D.C.C.R., pp. 57-81.

(23) La licéité du traitement est encore mieux spécifiée au point 4.3 du projet de recommandation du Conseil de l'Europe sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance. « Les données d'assurance peuvent être collectées et traitées : a) si la loi le prévoit notamment à des fins d'assurances obligatoires, b) pour la conclusion, la mise en œuvre et la cessation d'un contrat d'assurance auquel la personne

luée par rapport aux normes comprises dans les articles 5 et 95 (pour les données médicales) de la LAT. On y revient ci-dessous. La loyauté du traitement évoque, quant à elle, la transparence des opérations propres au traitement (24).

Les deuxième et troisième points du même paragraphe comprenant le principe de légitimité et de proportionnalité des traitements ont également leur importance : « les données à caractère personnel doivent être collectées, 2° pour des finalités déterminées, explicites et légitimes [...], 3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ».

Rappelons qu'il serait inadéquat, dans le cadre de la détermination de la légitimité et la licéité d'un traitement, de se référer à la notion de « droit de propriété ». Contrairement à la jurisprudence et à la doctrine ancienne, la vie privée informationnelle n'est pas conceptualisée en termes de propriété, mais bien en termes de « droits de la personnalité » ou de « liberté ». Cette approche ne garantit pas seulement la meilleure protection de la personne concernée, mais témoigne aussi d'un certain sens du réalisme, étant donné que l'on devra mettre en balance la vie privée de la personne concernée avec d'autres intérêts sociaux et libertés (voy. *infra* sous 3.2.) (25). Cet exercice de mise en balance des intérêts et libertés est encadré par les principes mentionnés ci-avant.

Le critère d'évaluation de la légitimité des informations demandées dans un questionnaire est mesuré par rapport à la finalité de celle-ci. Or, l'article 5 LAT stipule que la déclaration doit porter sur toutes les circonstances constituant pour

concernée est partie, ainsi que pour la préparation d'un tel contrat à la demande de la personne concernée, c) si la personne concernée ou son représentant légal ou une autorité ou toute personne ou instance désignée par la loi y a consenti, pour une ou plusieurs finalités d'assurance et pour autant que le droit interne ne s'y oppose pas, ou d) si ces données sont nécessaires à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement, à condition que ne prévalent pas les intérêts de la personne concernée ».

(24) « Cette transparence doit être assurée dès la collecte, notamment par le biais de l'obligation d'informer la personne concernée. Cette dernière doit savoir quel est le but d'utilisation des données, entre quelles mains elles se trouvent, à quelles fins elles sont communiquées, etc » : LEONARD, Th. et POULLET, Y., *l.c.*, J.T., 1999, p. 385.

(25) Consulter RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant, 1990; POULLET, Y., THUNIS, X., et LEONARD, Th., *La vie privée — une liberté parmi les autres*, Travaux de la faculté de droit de Namur, Tome 17, Bruxelles, Larcier, 231-277.

l'assureur « des éléments d'appréciation du risque ». Il s'ensuit du principe de proportionnalité que seulement les données qui sont de nature adéquate et pertinente à évaluer le risque peuvent être traitées. Les questions ne peuvent donc aucunement faire allusion à d'autres informations. En cas de contestation concernant la pertinence des questions, le législateur semble avoir mis la charge de la preuve auprès de l'assureur, ce qui nous paraît correct du point de vue de la protection du consommateur. La personne concernée aura d'ailleurs beaucoup de difficultés à prouver qu'une question est irrelevante pour l'évaluation du risque (26).

12. — Cependant, il est possible que le traitement de l'assureur ait certaines autres finalités légitimes. La norme simplifiée n° 16 de la CNIL peut être indicative à cet égard. Les fonctions, énumérées de façon limitative, sont les suivantes (27) :

a) traitement pour la passation et la gestion des contrats :

- l'étude des besoins spécifiques de chaque demandeur afin de proposer des contrats adaptés à ses risques;
- l'examen et le contrôle du risque;
- la tarification, l'émission des polices et des documents comptables, l'encaissement des primes ou cotisations, leur répartition éventuelle entre les coassureurs, le commissionnement des intermédiaires, la surveillance

(26) « Dans l'optique des auteurs du projet, si l'utilisation d'un questionnaire par l'assureur ne dispense pas le preneur d'assurance de l'obligation qui lui est imposée par l'alinéa 1^{er}, elle ne crée pas non plus en faveur de l'assureur la présomption que les circonstances sur lesquelles celui-ci a posé par écrit des questions précises qui enlèverait aux tribunaux leur pouvoir d'appréciation quant au caractère raisonnable de l'obligation du preneur d'assurance. Si l'assureur invoque le fait que le preneur a répondu erronément à des questions qui lui sont posées, il devra donc prouver que les circonstances faisant l'objet de ces questions constituent un élément d'appréciation du risque ». Exposé des motifs, Doc. Parl., Chambre, 1990-1991, n° 1586/1, pp. 16 et 17. Le Prof. Fagnart critique entre autres la volonté du législateur, en considérant que les assureurs ne perdront pas leur temps à poser par écrit des questions dont ils ne veulent pas connaître les réponses : FAGNART, J.-L., *op. cit.*, p. 82. On craint toutefois que cette critique parte d'un point de vue trop optimiste quant à la loyauté des traitements dans les secteurs commerciaux. L'augmentation des liens entre les assureurs et les autres acteurs du marché crée la possibilité de récolter une grande quantité d'informations, pour des finalités dépassant celle de l'évaluation du risque (voy. par exemple l'article dans le *Financieel Economische Tijd* du 26 août « GB, Fortis Bank en Shell lanceren samen getrouwheidskaart »).

(27) Délibération n° 81-04 du 20 janvier 1981 concernant les traitements automatisés d'informations nominatives relatifs à la passation, la gestion et l'exécution des contrats mis en œuvre par les organismes d'assurances, de capitalisation, de réassurance et d'assistance et par leurs intermédiaires (*Journal officiel* du 5 février 1981). Bien que cette norme date du 1981, les principes y reprise sont pour la plus grande quantité encore actuels.

des risques et les autres opérations techniques nécessaires;

b) traitement pour l'exécution des contrats :

- les opérations techniques nécessaires, notamment la détermination et le paiement des indemnités et prestations et, s'il y a lieu pour l'opérateur, leur collecte auprès des coassureurs, l'exécution des dispositions prévues au contrat et l'exercice des recours;

c) traitement pour l'élaboration des statistiques;

d) traitement pour l'établissement de sélections, parmi les clients de l'organisme, pour réaliser des actions de prospection et de promotion liées exclusivement aux activités propres à l'organisme;

e) traitement pour l'exécution des dispositions légales, réglementaires et administratives en vigueur.

Le texte du projet de la Recommandation du Conseil d'Europe mentionne à son tour également les finalités légitimes. Il s'agit de a) la préparation et la fourniture d'un contrat d'assurance, b) la collecte des primes et autres facturations, c) le règlement de demandes d'indemnisation ou d'autres prestations, d) la réassurance, e) la co-assurance, f) la prévention, la détection ou la poursuite des fraudes, g) la constatation, l'exercice ou la défense d'un droit en justice, h) le respect d'une autre obligation légale ou contractuelle spécifique, ou i) la gestion interne d'une compagnie d'assurance.

Certaines de ces finalités ne sont pas purement « internes », mais dans un souci d'être complet, elles sont mentionnées.

2.2. — Quant au traitement des données sensibles

13. — Le risque ne pourra être adéquatement apprécié pour certaines polices que si l'assureur dispose des informations à caractère sensible. Ainsi, l'estimation du risque pour la couverture RC automobile nécessite certes des informations quant à l'implication dans les accidents antérieurs ou concernant le passé judiciaire de la personne concernée. Dans le cadre de la conclusion d'une assurance-vie ou assurance de

santé, des informations relatives à celle-ci sont également pertinentes (28).

Le principe de solidarité inhérent à chaque système d'assurance plaide clairement en faveur de la légitimité du traitement des catégories des informations sensibles. D'ailleurs, les intérêts des autres assurés s'opposent à ce que l'un ou l'autre individu dissimule certains de ses antécédents judiciaires ou des informations médicales le concernant, ce qui amènerait inévitablement à augmenter le montant des primes pour les autres assurés du même 'pool'. Cet principe rationnel, ainsi que le principe de « self-selection » pourrait mener à la décomposition de l'assurance (29). La demande des informations sensibles se justifie donc non seulement par une finalité purement économique, mais également juridique, c'est-à-dire, qu'elle s'inscrit dans la pensée de l'obligation de prudence.

14. — Il est connu que la LAT confirme dans son article 95 le fait que l'assureur peut requérir des informations médicales, à l'exception des informations génétiques (30). Toutefois, la loi reste muette quant à l'acquisition des autres catégories d'informations sensibles.

Il nous semble qu'en formulant une réponse complète, on doit prendre en considération les dispositions de la LVP.

Ce dernier texte contient un régime spécifique à propos des données sensibles, qui sont classées en trois catégories, notamment les données sensibles « tout court » (art. 6 LVP), les don-

(28) Voy. l'A.R. du 17 décembre 1992 relatif à l'activité d'assurance sur la vie, *M.B.* 31 décembre 1992.

(29) Voy. BERGKAMP, L., *op. cit.*, p. 48.

(30) Art. 95 : « Le médecin choisi par l'assuré remet à l'assuré qui en fait la demande les certificats médicaux nécessaires à la conclusion ou à l'exécution du contrat. Les examens médicaux nécessaires à la conclusion et à l'exécution du contrat ne peuvent être fondés que sur les antécédents déterminant l'état de santé actuel du candidat assuré et non sur des techniques d'analyse génétique propres à déterminer son état de santé futur. Pour autant que l'assureur justifie de l'accord préalable de l'assuré, le médecin de celui-ci transmet au médecin-conseil de l'assureur un certificat établissant la cause du décès ». Voy. NYS, H., « Van afkomst naar toekomst? Juridische grenzen van erfelijkheidsonderzoek bij verzekeringen », *Bull. Ass.*, 1992, 209-219; BOULANGER, M.-H. et DHONT, J., « Protection de la vie privée et données génétiques : quelques considérations », dans E. MONTERO (éd), *Droit des Technologies de l'Information — Cahiers du Centre de Recherches n° 16*, Bruylant, Bruxelles, 1999, 173-196; JEGER, N., CAUWENBERGH, P., « Individuele levensverzekeringen 'overlijden' en erfelijkheidsonderzoek : een kritische analyse van de artikelen 5 en 95 van de wet van 25 juni 1992 op de landverzekeringsovereenkomst », *Rev. Dr. Santé* 1996-97, 239-256.

nées « relatives à la santé » (art. 7 LVP), et les données « judiciaires » (art. 8 LVP). On pourrait déceler dans cette protection particulière une application du principe de proportionnalité : certaines informations risquant d'être traitées de manière illégitime ou illégale, ou celles dont le traitement présente un plus grand impact sur des libertés fondamentales, méritent une meilleure protection.

On s'attarde sur la question de la légalité du traitement de la deuxième et de la troisième catégorie, vu que celles-ci méritent plus d'attention dans le cadre des assurances (31).

2.2.1. Traitement des données « relatives à la santé »

15. — Bien qu'une lecture conjointe des articles 5 et 95 LAT laisse entrevoir que le traitement des données relatives à la santé par l'assureur soit directement légitime, la vérité juridique ne se comprend qu'en termes plus nuancés.

En date du 25 juin 1992 et donc avant l'existence de LVP (première version), le secret médical dans sa conception absolue formait un obstacle à la communication des informations par le médecin traitant au médecin de la compagnie d'assurances. Selon cette conception, le patient ne pouvait pas délier le médecin de son secret. L'article 95 paraît légitimer le fait que l'assureur puisse recevoir, et donc traiter ces informations, pour autant que la théorie relativiste du secret soit instaurée par cette disposition.

Toutefois, à l'époque, en l'absence de norme législative ou réglementaire relative à la protection des données à caractère personnel rien n'empêchait la compagnie d'assurance de récolter des informations médicales directement auprès de l'assuré/preneur d'assurance. La LAT ne se prononce donc pas sur la légalité du traitement même — plus particulièrement l'enregistrement et la conservation — des données relatives à la santé, sinon de manière indirecte dans la mesure où elle pourra constituer un des facteurs qui devront être pris en considéra-

(31) Les données tombant dans la première catégorie sont les suivantes : celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la vie sexuelle. Le traitement de ces données est interdit, sauf les exceptions prévues par la loi.

tion afin d'évaluer la légitimité de la finalité du traitement. La pondération des intérêts mis en jeu par rapport au traitement des données n'est pas présente dans ce texte. Dans cette ligne d'idées, on est d'avis que cette dernière loi n'est pas une *lex specialis* dérogeant à toutes les normes inscrites dans la LVP (32). Les dispositions quant au traitement des données sensibles sont applicables aux traitements réalisés par les compagnies d'assurances.

De plus, cette dernière loi règle certains aspects d'une liberté constitutionnelle et se présente comme une loi-cadre par rapport à laquelle les règles sectorielles doivent être interprétées.

Il ressort de l'article 7 LVP que le traitement de données relatives à la santé (33) est en principe interdit. Des exceptions sont cependant formulées, autorisant le traitement dans certaines circonstances et sous certaines conditions. Parmi les onze exceptions énumérées, il semble qu'une seule puisse être

(32) Cette question se pose de façon plus délicate dans le secteur de la protection des consommateurs, consultez POULLET, Y. et LEREBRE, A., « La vie privée et crédit à la consommation, protéger le consommateur ou sa vie privée : un choix difficile », Edition Jeune Barreau de Bruxelles, 1997, pp. 103-134.

(33) Là où le législateur adhère à la notion de « données médicales » sous l'ancienne version de la loi, on parle désormais de « données relatives à la santé ». Le nouvel article 7 de la loi ne définit plus ce qu'il faut entendre par ce type de données. Précédemment, on entendait par « données médicales » « toutes données à caractère personnel dont on peut déduire une information sur l'état antérieur, actuel ou futur de la santé physique ou psychique, à l'exception des données purement administratives ou comptables relatives aux traitements et aux soins médicaux ».

L'exposé des motifs contient des explications totalement contradictoires. Il invite d'abord à reconnaître une portée plus étroite à la donnée « relative à la santé ». Alors que les données qui « révèlent » une information sensible visent toute information sensible « déduite » de la donnée — comme visé précédemment dans la définition de la donnée médicale — celles qui sont seulement « relatives » à la santé doivent « se rapporter » à ces informations. Toutefois, le mémoire déclare que les données relatives à la santé seraient une catégorie de données plus large que les données médicales (Chambre des représentants, n° 1566/1, 1997-1998; ci-après : « Exposé des motifs »).

On est d'avis que les « données relatives à la santé » couvrent une réalité plus ample que la notion de donnée médicale dans la loi précédente. Aussi la recommandation R (97)5 du Comité des Ministres du Conseil d'Europe, qui utilise encore l'expression « données médicales » contient une définition large : toutes les données à caractère personnel relatives à la santé d'une personne. Elle (la définition) se réfère également aux données ayant un lien manifeste et étroit avec la santé ainsi qu'aux données génétiques. Par analogie avec la notion de « donnée personnelle », où on ne doit pas être à même de déduire des informations d'une personne identifiée ou identifiable d'une donnée, il suffit ici que l'information soit « relatée » ou « concerne » la santé d'une personne. En conséquence, non seulement les informations médicales « dures » tomberont sous la définition, mais également celles qui reçoivent une connotation médicale par le contexte (voy. DHONT, J. et POULLET, Y., *De verwerking van medische persoonsgegevens voor wetenschappelijke en statistische doeleinden*, D.W.T.C., 1998, pp. 28 et s.).

retenue pour rendre le traitement légitime, à savoir « le consentement écrit » (34)/(35).

L'exigence du consentement « écrit » révèle l'exigence d'un caractère « plus certain » du consentement d'une personne au traitement de données personnelles particulièrement sensibles. Il nous semble que le consentement n'est respecté que si la proposition d'assurance ou le contrat fait la distinction entre une signature présentant l'accord au traitement des informations et la signature confirmant l'accord de l'offre.

Même si le consentement écrit au traitement a été donné, il peut être retiré en principe à tout moment (article 7, § 2 a LVP). Bien que cette formule de « opt-out » pose relativement peu de problèmes dans un contexte thérapeutique marqué par une relation de confiance entre professionnel de la santé et patient, l'application dans le cadre d'un traitement pour des finalités d'assurance devient par contre moins évidente. La compagnie d'assurance aura besoin de ces informations non seulement au moment de la conclusion du contrat, mais également pendant l'exécution, par exemple pour réorienter les prix des primes...

Les travaux préparatoires sont également peu clairs quant à l'utilisation dans le secteur des assurances des données relatives à la santé (36). On voit mal comment la personne concer-

(34) Voy. article 7 § 2 a) LVP. Le Roi peut déterminer, par arrêté délibéré en Conseil des ministres après avis de la Commission de la protection de la vie privée, dans quels cas l'interdiction de traitement de données relatives à la santé peut être levée par le consentement écrit de la personne concernée. Cet A.R. n'est pas encore pris.

(35) La loi mentionne encore une autre exception qui semble de première vue être d'importance : « Le traitement serait admissible lorsque le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice (voy. article 7 § 2, i LVP) ». Bien que ce paragraphe légitime le traitement dans un contexte contentieux, il ne justifie pas le traitement pour l'évaluation du risque en phase précontractuelle, ou l'enregistrement et la conservation après la conclusion de la convention. Ceci implique d'ailleurs une autre finalité. L'exposé des motifs n'anticipe à aucun moment ce problème, sauf dans le contexte de la même exception à l'interdiction principale de traitement des données judiciaires : « [...] Comme dans l'actuel article 8, une exception a été prévue pour la gestion du contentieux propre à la personne concernée ou pour des avocats ou d'autres conseils juridiques qui doivent traiter des données judiciaires afin de défendre les intérêts de leurs clients. La suggestion de la Commission de la protection de la vie privée (n° 30/96, § 21) de limiter cette exception aux conseils juridiques qui sont liés par « le secret professionnel sanctionné pénalement », n'est pas suivie dans le projet. En effet, pour un certain nombre de cas concrets où des dossiers judiciaires sont traités par des préposés des compagnies d'assurances ou des organisations syndicales représentatives des travailleurs, la notion du « secret professionnel » est probablement trop stricte » (Exposé des motifs, p. 43). Ce principe rationnel vaut pour la même exception des autres catégories des données sensibles, mais, comme nous l'avons dit, ne sert qu'à une finalité contentieuse.

(36) Exposé des motifs, pp. 38 et s.

née peut se prévaloir de ce droit sans annuler les liens contractuels avec l'assureur.

Les exceptions relatives à l'interdiction de traitement de données relatives à la santé ne sont admises que si le traitement de ces données est effectué sous la responsabilité d'un professionnel des soins de santé (37), sauf en cas de consentement écrit de la personne concernée ou de nécessité pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée (38).

Dans l'hypothèse où les informations médicales sont communiquées, avec l'accord préalable (39) de l'assuré, de son médecin traitant (ou médecin de son choix) au médecin assureur, il y a peu de problèmes, vu que ces informations sont directement gérées sous la responsabilité de ce dernier (tenu d'ailleurs par le secret médical).

Vu que sous le régime de la nouvelle loi relative à la protection des données la « collecte » doit être qualifiée de « traitement » (40), on se pose la question de savoir si elles peuvent être récoltées par un intermédiaire d'assurances, ou un préposé qui n'a pas la qualité d'un professionnel des soins de santé. Est-ce que la notion de « responsabilité » du professionnel de la santé, s'étend si loin et peut raisonnablement comprendre la phase précontractuelle ?

Les travaux préparatoires ne suggérant rien, il nous semble qu'une interprétation aussi large de la notion de « responsabilité » minerait la disposition de toute signification. Il est, par

(37) La notion de « professionnel de la santé » n'est pas définie dans la loi, mais est certainement plus large que les termes « praticiens de l'art de guérir ». L'exposé des motifs relève qu'en pratique, la notion de « praticiens de l'art de guérir » était trop limitée (Exposé des motifs, p. 38). L'évolution de la médecine révélant davantage une pratique « en groupe » a certes mené à un assouplissement de cette règle, ce qui est d'ailleurs insinué par l'exposé des motifs : « professionnel de la santé » correspondrait « à un concept vaste qui fait référence à l'ensemble des personnes qui prestent des soins de santé à l'égard d'autres personnes dans l'exercice de leur profession ». Voy. pour une critique LEONARD, Th. et POULLET, Y., *l.c.*, p. 388.

(38) Voy. article 7, § 4 LVP.

(39) Cet « accord préalable » doit être un « consentement libre et éclairé » au sens de la LVP (voy. article 1^{er}, § 8), vu qu'article 7 § 5 LVP prévoit que les données à caractère personnelles relatives à la santé sont collectées auprès de la personne concernée. Elles ne peuvent être collectées auprès d'autres sources qu'à condition que la collecte soit conforme aux §§ 3 et 4 et qu'elle soit nécessaire aux fins du traitement ou que la personne concernée ne soit pas en mesure de fournir les données elle-mêmes. Le § 4 prévoit justement l'exception par « consentement ».

(40) Voy. article 1^{er}, § 2 LVP.

conséquent, tout à fait justifié que le consentement du preneur d'assurance ou de l'assuré couvre aussi le fait que les informations sont récoltées par des non-professionnels des soins de santé. De surcroît, la compagnie d'assurances devra garantir des mesures d'organisation et devra veiller au respect de ces mesures, notamment par la stipulation de mentions contractuelles (41).

16. — Un commentaire de la légitimité des données relatives à la santé ne peut pas faire abstraction d'une réflexion sur le secret médical. Ce sujet donne à lui seul lieu à un commentaire étendu dépassant le cadre de cet article. On voudrait n'en faire qu'une note succincte.

L'article 95 LAT, ainsi que la littérature en la matière confirment que le patient peut délier le médecin de son secret (42). L'assureur se réservera en réalité le droit de subordonner son acceptation quant au risque à assurer, à l'obtention, auprès du médecin traitant de l'assuré, d'informations médicales complémentaires. Cet article, qui sert une finalité principalement économique (43), implique-t-il que le médecin peut informer son patient, candidat preneur d'assurance, de toutes les informations que la compagnie demande ? Est-ce que la relation de confiance n'est pas mise en péril si le médecin traitant est dégradé à « un auxiliaire des compagnies d'assurances » ?

Il nous paraît que même en étant délié, le médecin, devant mettre en balance les différents intérêts à la cause, devra dans certains cas, maintenir ce secret. C'est en tout cas la règle aux Pays-Bas (44).

(41) Voy. article 16 LVP.

(42) Voy. BINON, J.-M., « Assurance-vie règles générales et droits du preneur », *op. cit.*, Collection Droit des Assurances n° 6, pp. 256 et s.; COLLE, Ph., *op. cit.*, pp. 158 et s.; HENNAU-HUBLET, C., « Là où la preuve en matière d'assurance se heurte à la règle du secret médical », note sous Cass., 19 décembre 1994, *Rev. Dr. Santé*, 1996-97, pp. 257-261.

(43) « [...] Il faut bien constater que ce sont des raisons exclusivement économiques qui ont justifié l'article 95 en matière d'assurances de personnes. Il fut adopté à un moment où les contrats d'assurance hospitalisation tendaient à se développer au point de menacer la santé financière des compagnies d'assurance », HENNAU-HUBLET, C., *l.c.*, p. 259.

(44) DE JONG, E.C.M., « Mogen nabestaanden het dossier van een overledene inzien », *Medisch Contact*, 1998, 1017-1020.

Plus précisément, on accepte que le secret médical inscrit dans l'article 458 Code Pénal serve à la fois une finalité micro-juridique et macro-juridique (45). La finalité micro-juridique de l'intérêt individuel du patient se dissimule derrière la pensée que l'individu doit pouvoir se confier sans réserve afin de recevoir les soins qu'exige son état, quelle qu'en soit la cause. Il doit également pouvoir compter sur le fait qu'il sera soigné en toute confiance. La finalité macro-juridique de l'intérêt général est également de mise. Le secret protège également la société qui a intérêt à ce que chacun puisse en toute confiance et librement recevoir des soins. Il est clair que ces deux intérêts sont liés et ne peuvent être envisagés de manière distincte.

La théorie relative au secret met davantage l'accent sur les intérêts de l'individu. Ce faisant, le consentement du patient à une révélation de ses données fait office de justificatif à l'écartement du devoir de silence (46). La théorie relative étant validée par le législateur, on pense qu'il sera tout de même nécessaire de vérifier dans chaque cas d'espèce si l'intérêt général ne s'oppose pas à ce que l'on fasse exception au devoir de silence. Concrètement, il s'agira d'examiner d'une part, si la révélation totale ou partielle du secret est le seul moyen de protéger l'intérêt légitime du patient et si aucun moyen ne peut être utilisé et, d'autre part, si la défense de l'intérêt particulier du patient est plus importante que l'accomplissement de l'intérêt général.

Bien que le médecin ne soit plus punissable — dans le contexte des assurances — quand il communique les informations demandées, il nous semble que le médecin ne peut pas être *obligé* de lever le secret là où l'intérêt de son patient ou la confiance réciproque est menacée. Dire le contraire, serait fermer les yeux pour la réalité médicale.

(45) Voy. F. DEWALLENS, « De contextualisering van het medisch geheim : een goedbedoelde poging voor meer rechtszekerheid met een omgekeerd effect », dans R. STOCKMAN (éd.), *Het beroepsgedrag in de zorgverleningssector — een confrontatie tussen recht en praktijk*, Antwerpen — Groningen, Intersentia Rechtswetenschappen, 1998, 82-83; BOU-LANGER, M.-H. et DHONT, J., « Protection de la vie privée et données génétiques : quelques considérations », dans E. MONTERO (éd.), *Droit des Technologies de l'Information — Cahiers du Centre de Recherches n° 16*, Bruylant, Bruxelles, 1999, pp. 183 et s.

(46) La théorie relative a été reconnue par le Cour de Cassation, voy. Cass., 9 février 1988, *Pas.*, I, 1988, 662; Cass., 29 octobre 1991, *Pas.*, I, 1992, 197.

Dans un avis du 16 novembre 1996, le Conseil national de l'Ordre des Médecins a estimé qu'il serait préférable que le médecin traitant ne prenne pas en charge la mission de rapporteur des constatations à l'assureur et estime qu'il est également recommandé que le médecin traitant ne procède pas lui-même à l'examen médical du candidat assuré.

De plus, suivant le principe de proportionnalité, l'assureur peut seulement requérir les informations qui sont pertinentes pour la police concernée (art. 4 LVP).

2.2.2. Le traitement des données judiciaires

17. — L'évaluation du risque nécessitera dans certaines cas la récolte d'informations d'ordre judiciaire (p.ex. dans le contexte RC-automobile : reconnaissance de responsabilité, condamnation pour ivresse au volant, etc.). On verra plus loin que cette catégorie a également son importance dans le cadre des mutuelles des informations en vue de distinguer les fraudeurs des non-fraudeurs.

18. — Dans son article 8, la LVP interdit en principe le traitement des données judiciaires à caractère personnel.

Contrairement à la première version de la loi, le législateur a préféré ne pas inclure dans la loi une liste détaillée des données judiciaires et de partir d'une définition plus générale, comme le fait la directive. Tombe en effet sous le champ d'application de l'article 8 « le traitement de données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions ou à des sanctions administratives, ou à des mesures de sûreté » (47).

L'exposé des motifs précise encore que « la notion de » suspicions, poursuites ou des condamnations relatives à des infractions » montre que l'article 8 ne s'applique pas uniquement aux condamnations pénales mais également aux données dont

(47) Voy. article 8 LVP. Cette définition élargit celle présente dans la directive 95/46/CE. Cette dernière ne vise ni les données relatives aux suspicions et aux poursuites, ni celles relatives aux « litiges » soumis aux cours et tribunaux se limitant, dans ce dernier cas, aux données relatives aux jugements civils.

il ressort qu'une personne est soupçonnée ou poursuivie pour un délit » (48).

Hormis le fait que la définition laisse beaucoup de questions sans réponses (49), on constate qu'en incorporant des suspicions relatives à des infractions, la définition est devenue très large. La Commission de la protection de la vie privée a toujours estimé que les notions de « suspicion » et « d'implication dans une infraction » devaient s'interpréter de manière large étant donné la présomption d'innocence et le grand risque pour la vie privée des personnes concernées que le traitement de pareilles données engendre. Ainsi, doit tomber sous ce vocable la notion de « personne à surveiller » du système Schengen. Il en va de même concernant des données *douces* ou de simples « présomptions » sans preuves tangibles (50).

A partir du moment où une donnée est traitée dans le contexte d'une instruction ou dans le cadre d'une enquête judiciaire et qu'elle a trait à des infractions pénales, elle sera qualifiée de « judiciaire ». En sera-t-il ainsi dans le cas d'enregistrements d'informations suspectieuses par des acteurs privés (banques, entreprises)? Ou est-ce que cette qualité particulière n'est attribuée qu'à partir du moment où la finalité d'un tel traitement consiste précisément à communiquer les données aux instances judiciaires?

On est d'avis qu'en liant la qualité de la donnée à la finalité mentionnée ci-avant, on déplace le problème dans la mesure où il suffit qu'il n'y ait pas communication pour éviter la protection de la LVP. Les informations quant aux suspicions de fraudes pénales tenues par des acteurs privés bénéficient de cette protection (51).

19. — Les exceptions sur l'interdiction principale sont encore plus limitées que dans le cas du traitement des données relatives à la santé.

(48) Exposé des motifs, p. 42.

(49) A partir de quel moment les données relatives aux litiges soumis aux cours et tribunaux sont estimées être d'ordre judiciaire? Dès la citation ou dès la comparution? Est-ce que les instances disciplinaires sont visées par l'article 8 de la loi? S'agit-il obligatoirement de procédures contentieuses? Quid des procédures gracieuses?

(50) Avis 08/93, n° 18.

(51) LEONARD, Th. et POULLET, Y., *l.c.*, p. 388.

Des cinq exceptions, on en commentera brièvement deux. L'interdiction de traiter les données judiciaires n'est pas applicable aux traitements effectués :

« [...] »

- b) par d'autres personnes [que des autorités publiques ou officiers ministériels] lorsque le traitement est nécessaire à l'exercice de leurs tâches;
- c) par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige. [...] ».

On remarque que la loi exclut la possibilité de traiter des données judiciaires avec le consentement de la personne concernée.

20. — Peut-on considérer que l'article 5 LAT soit une base légale suffisante dans le sens du point b précité? On se pose la question de manière plus précise : est-ce que l'article 5 pose une finalité assez bien déterminée légitimant le traitement des données judiciaires?

Il nous paraît qu'une fois de plus la réponse doit être formulée en termes nuancés.

La LAT prévoit l'obligation dans le chef du preneur d'assurances de fournir toutes les informations qu'il doit raisonnablement considérer comme constituant pour l'assureur des éléments d'appréciation du risque. Il est évident que parmi ces informations, il y aura sans doute des données pouvant être qualifiées de nature « judiciaire ». On pourrait donc déduire que l'obligation du preneur correspond au droit d'obtenir et de traiter ces informations. De plus, on a déjà indiqué que l'assureur doit assumer une obligation de prudence et de bonne gestion, le risque n'ayant pas été bien estimé ayant des conséquences pour les autres assurés.

D'autre part, l'obligation d'évaluer le risque n'est pas *fixée* de façon positive dans la loi. Contrairement à l'appréciation de la finalité d'un traitement sous l'article 4 § 1, 2° LVP, où la déclaration obligatoire constitue un des paramètres pour conclure à la légitimité du traitement, il apparaît ici que la finalité concernant les données sensibles doit être formulée de façon positive par une loi matérielle. De plus, les exceptions

doivent être interprétées de façon restrictive, vu qu'il s'agit d'exceptions aux dispositions qui protègent des intérêts touchant aux libertés fondamentales des personnes concernées. De plus, l'esprit de la loi reproduit par l'exposé des motifs, témoigne d'une volonté stricte et très protectrice (52).

La frontière entre les deux interprétations est très étroite, et beaucoup de choses dépendront de quel côté de cette frontière on se trouve dans la réalité.

Dans le cadre de l'évaluation de la légitimité du traitement, le traitement des données judiciaires se justifie partiellement par rapport à l'article 5 LAT, dans la mesure où cette catégorie particulière de données reste interne à la compagnie d'assurance (donc strictement pour l'évaluation du risque). Bien que l'article 5 de la loi précitée laisse éventuellement entrevoir une obligation dans le chef de l'assureur, cette obligation n'existe pas pour un tiers, plus particulièrement une mutuelle d'informations. Interpréter cet article de telle manière irait à l'encontre du principe de proportionnalité inhérent aux articles 2 et 4 LVP.

En ce qui concerne le point c), il faut rappeler que bien que les informations judiciaires puissent être traitées par les assureurs pour la gestion de leurs propres contentieux, ceci ne justifie pas que ces données soient récoltées dans l'absence de chaque litige.

21. — Enfin, dans l'hypothèse où les données judiciaires pourraient exceptionnellement être enregistrées et traitées, les personnes effectuant le traitement sont tenues au secret professionnel (article 8, § 3 *jo.* article 16 LVP).

22. — On en conclura que le traitement des données judiciaires n'est pas évident, le législateur n'ayant apparemment pas suffisamment examiné les diverses hypothèses des demandes de la réalité économique et sociale.

2.3. — *Marketing Direct*

23. — Les compagnies d'assurances, à l'instar des banques, disposent d'un grand nombre d'informations sur leurs clients.

(52) Exposé des motifs, pp. 42-43.

Ces informations peuvent servir notamment à maximaliser le chiffre d'affaire. Les gains existeront dans la vente des informations ou dans un « recyclage » pour l'offre de nouveaux produits, éventuellement après un procès de « data-mining ». On ne peut nier que le client en tire également profit vu qu'il est tenu au courant de toutes les offres intéressantes souvent adaptées à ses propres besoins et moyens économiques. Ces données à caractère personnel vont cependant circuler à l'insu de la personne concernée. La transparence est parfois minime, et avec le renforcement des liens de coopération entre entreprises et l'intensification de l'internationalisation de ceux-ci, la vie privée des personnes concernées se voit menacée (53).

24. — La légalité de l'utilisation des données à caractère personnel est jugée par rapport au principe de finalité (article 4 § 1 LVP). Ainsi, le « marketing direct » sera en principe considéré comme une finalité légitime (54). Toutefois, les informations que le client a données lors de la conclusion du contrat servent en principe une autre finalité (évaluation du risque; administration). Par conséquent, si le client n'était pas au courant d'une telle utilisation potentielle, le consentement postérieur de celui-ci s'impose.

Nous estimons que la compagnie a le droit de s'adresser à son client sur base des informations qu'elle détient pour lui offrir des nouveaux produits (finalité purement interne) (55). Du moment que la compagnie fait appel à un tiers pour approcher le client ou veut commercialiser les données, le consente-

(53) Voy. WALRAEVEN, M., *Privacy geschand*, Universitaire Pers Leuven, 1999.

(54) Sous le régime de la LVP est plus large que « prospection » : Le texte français du projet utilise la notion « marketing direct » au lieu de la notion de « prospection » utilisée dans la version française de la directive. En effet « marketing direct » (en Allemand : « Direktwerbung ») couvre une gamme d'activités beaucoup plus large que la seule prospection et englobe toute forme d'offre personnalisée non seulement de clients potentiels mais également de clients existants (marketing de rétention). Le terme « marketing direct » est également celui qui est employé dans la version française de la Recommandation qui a été adoptée par le Conseil de l'Europe à ce sujet; Exposé des motifs, p. 47.

(55) On pourrait contester ce point de vue se référant à la décision du Cours d'Appel d'Anvers du 3 mai 1999 (1994/AR/3319). Toutefois, il nous paraît qu'il est opportun de distinguer cette affaire de l'hypothèse d'une utilisation dans le contexte preneur d'assurances-assuré. Dans l'affaire mentionnée ci-avant, il s'agissait d'une banque qui utilisait des informations générées lors de transcriptions financières de ses clients. La banque constatait que son client versait des primes d'assurance à un assureur-concurrent et se dirigeait ensuite vers le client afin de lui offrir des proposition d'assurances. Le président de la Cour d'Appel a estimé que le principe de finalité a été violé ce qui constitue une pratique de commerce déloyale.

ment de la personne concernée sera obligatoire, sauf dans le cas où la personne concernée en a été informée lors la conclusion du contrat (voy. article 4 § 1, 2 LVP — en ce qui concerne l'obligation d'informer, cf. *infra* 2.4.1).

Dans l'hypothèse où la personne concernée a été informée au moment de la proposition de l'assurance, la compagnie d'assurance aura le droit d'utilisation pour le « marketing direct ». Le projet de recommandation du Conseil de l'Europe sur la protection des données à caractère personnel et traitées à des fins d'assurance stipule : « 4.10. Pour autant que la personne concernée en ait été informée et ne s'y soit pas opposée, le responsable du traitement peut utiliser, à des fins de démarchage et de promotion de la gamme de service à sa disposition, les données collectées et enregistrées à des fins d'assurance ».

La LVP ne consacre donc pas explicitement un système de « opt-in » lors du traitement des données pour des finalités de direct marketing, *pour autant que* cette dernière finalité soit compatible avec les finalités pour lesquelles les données ont été initialement récoltées.

25. — A la lumière de la Directive 95/46/CE, un droit d'opposition est cependant explicitement attribué à la personne concernée : « Lorsque les données à caractère personnel sont collectées à des fins de direct marketing, la personne concernée peut s'opposer, gratuitement et sans aucune justification, au traitement projeté de données à caractère personnel la concernant. En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut plus porter sur ces données. » (article 12 § 1 LVP).

Pour que ce droit soit effectif, il faut que le client en soit suffisamment informé, ce qui est d'ailleurs explicitement prévu par l'article 9 LVP. Ceci impliquera qu'il soit informé non seulement des finalités génériques, mais des finalités plus spécifiques, ainsi que de toutes les informations pour garantir la loyauté du traitement (article 4 § 1, 1° LVP). Conformément au point 4.10 du projet de Recommandation du Conseil de l'Europe l'assureur devrait idéalement informer la personne concernée « du fait que son refus de consentement ou son opposition à l'utilisation de ses données pour les fins de démarchage et de promotion ne portera pas atteinte à la décision de

lui fournir une couverture par l'assurance ou de bénéficier d'une couverture par l'assurance déjà accordée ».

Notons encore que le traitement des données sensibles pour des finalités de « marketing direct » doit être estimé comme étant illégal, et ce même avec le consentement de la personne concernée, vu que la finalité sera dépourvue de sa légitimité. Ceci ressort également du projet de Recommandation cité ci-dessus : « Cependant si le traitement porte sur des données sensibles, le consentement explicite de la personne concernée est nécessaire pour autant que le droit interne ne s'y oppose pas ».

2.4. — *Aperçu des obligations du responsable de traitement*

26. — La compagnie d'assurance doit en sa qualité de « responsable du traitement » respecter les obligations qui sont stipulées par la LVP. Il s'agit plus particulièrement de l'obligation d'information de la personne concernée (article 9 LVP), de garantir le droit d'accès, le droit de rectification et le droit d'opposition (article 10 et 12 LVP), de respecter l'interdiction des décisions automatisées (article 12bis LVP) et de faire une déclaration auprès de la Commission de la protection de la vie privée (article 17 LVP).

2.4.1. *Information de la personne concernée (l'assuré, le preneur d'assurances ou tiers)*

27. — Selon le principe de transparence, la personne concernée doit être bien informée des modalités du traitement des données le concernant. Ainsi, l'article 9 § 1 LVP prévoit que « le responsable du traitement ou son représentant doit fournir à la personne concernée auprès de laquelle il obtient les données la concernant et au plus tard au moment où ces données sont obtenues, au moins les informations énumérées ci-dessous, sauf si la personne concernée en est déjà informée » :

- a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant;
- b) les finalités du traitement;

- c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de « direct marketing »;
- d) d'autres informations supplémentaires, notamment :
 - les destinataires ou les catégories de destinataires des données,
 - le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse,
 - l'existence d'un droit d'accès et de rectification des données la concernant;
 sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont obtenues, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données;
- e) d'autres informations déterminées par le Roi en fonction du caractère spécifique du traitement, après avis de la commission de la protection de la vie privée.

La nécessité de procurer des informations supplémentaires (point d) dépendra des risques accrus découlant du traitement particulier (56). On pense entre autres au traitement de données sensibles ou au fait que le traitement se déroule en partie à l'étranger (57).

Ces informations peuvent en effet, pour plus de commodité, être mentionnées sur la proposition d'assurance et sur la déclaration de sinistre.

Lorsque les données n'ont pas été obtenues auprès de la personne concernée, le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données, fournir à la personne concernée au moins ces mêmes catégories d'informations, sauf si la personne concernée en est déjà informée

(56) Voy. LEONARD, Th. et POULLET, Y., *l.c.*, p. 389.

(57) Voy. également point 5 du projet de Recommandation du Conseil de Ministres. Point 5.5 ajoute encore pour les personnes légalement incapables : « Si la personne concernée est une personne légalement incapable et n'est pas en mesure de se déterminer librement, et si le droit interne ne lui permet pas d'agir en son propre nom, l'information doit être donnée à la personne pouvant agir légalement dans l'intérêt de la personne concernée. Si elle est en mesure de comprendre, la personne légalement incapable doit être informée avant que les données qui la concernent soient collectées ou traitées ».

(article 9 § 2 LVP). Il existe une exemption, entre autres, lorsque l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

2.4.2. Garantir le droit d'accès, et le droit de rectification

28. — Toute personne concernée (assuré, preneur ou tiers) peut, en prouvant son identité, obtenir la confirmation que les données la concernant sont ou ne sont pas traitées. Elle peut également obtenir des informations sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories des destinataires auxquelles les données sont communiquées (article 10 § 1 a LVP).

Notons que la communication doit se faire de façon compréhensible. De plus, l'origine des données doit être communiquée.

La demande se fait par écrit. Les renseignements sont communiqués sans délai et au plus tard dans les quarante-cinq jours de la réception de la demande.

Concernant l'exercice du droit d'accès aux données relatives à la santé, la loi a prévu un régime spécifique. La communication peut être obtenue soit par l'intermédiaire d'un professionnel des soins de santé, soit directement par le responsable (l'article 10 § 2) (58). Il est préférable que l'accès soit réalisé par l'intermédiaire d'un professionnel de la santé, si l'information est susceptible de nuire à la santé de la personne concernée (exception thérapeutique). On pense plus particulièrement à l'hypothèse où des informations relatives à la santé sont obtenues par le médecin assureur d'un médecin choisi (ou traitant) dans le cadre de l'article 95 LAT (59).

Enfin, la personne concernée a le droit d'obtenir sans frais la rectification de toute donnée à caractère personnel qui

(58) A la demande du responsable du traitement ou de la personne concernée, la communication peut être effectuée par l'intermédiaire d'un professionnel des soins de santé choisi par la personne concernée (article 10, § 2, 2° al.).

(59) Pour la problématique du droit d'accès par rapport aux données relatives à la santé DHONT, J. et POULLET, Y., « Het Algemeen Medisch Dossier : een correcte afweging tussen staatsveiligheid en de vrijheid van de zorgverlener en de privacy van de patiënt? », *Rev. Dr. Santé*, 1999-2000, pp. 246-254.

serait inexacte. Elle dispose également du droit d'obtenir sans frais la suppression ou l'interdiction de l'utilisation de toute donnée à caractère personnel la concernant *qui, compte tenu du but du traitement, est incomplète ou non pertinente ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui a été conservée au-delà de la période autorisée* (article 12, § 1 LVP).

2.4.3. Décisions individuelles automatisées

29. — Selon l'article 12bis LVP, une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destinées à évaluer certains aspects de sa personnalité (60).

Dans les assurances, certaines pratiques de décisions automatisées peuvent être remises en question : le calcul des primes, la décision d'accorder ou de refuser certaines polices, etc.

Toutefois, la loi prévoit deux exceptions. L'une prévoit que la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance, ce contrat ou cette disposition devant en effet contenir des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de l'intéressé. Ce dernier pourra au moins faire valoir son point de vue (61). L'exposé des motifs ne spécifie pas ce qu'il faut entendre par « dans le

(60) L'exposé des motifs stipule que « cette disposition doit éviter que, sans aucune intervention humaine, des décisions soient prises directement sur la base d'un résultat d'un traitement automatisé ». Il est encore déterminé que « on respecte donc la disposition lorsque, entre l'obtention du résultat du traitement par ordinateur et la prise de décision, il y a au moins une intervention humaine minimale » (Exposé des motifs, p. 52). Leonard et Poulet précisent encore : « L'interdiction vaut donc non seulement lorsqu'il n'y a aucune intervention humaine mais également lorsque la décision est transmise par l'intermédiaire d'une personne sur la seule base du résultat du traitement. L'intervention humaine doit donc avoir pour conséquence la prise en compte d'autres éléments que les résultats de traitement. En pratique, la charge de la preuve pèsera sur la personne concernée par les données. Elle sera aidée par le fait que l'accès porte également sur la logique qui sous-tend le traitement. On peut se demander également si la logique du raisonnement qui sous-tend la décision prise sur la base non exclusive du traitement ne devrait pas être expliquée à la personne concernée sur la base d'obligation d'information. Sans cela, on peut craindre que la personne concernée ait de sérieuses difficultés à prouver que les conditions d'application de la disposition sont remplies »; LEONARD, Th. et POULET, Y., *l.c.*, p. 391.

(61) Article 12bis, deuxième alinéa de la LVP.

cadre d'un contrat ». L'exception comprend-elle également la phase précontractuelle ? On ne le pense pas. Quelle serait, dans l'hypothèse inverse, la volonté du législateur quand il précise que le libellé de l'article dans le cas d'espèce « vise des systèmes de décisions automatisées générant des scores et/ou autres résultats qui ont un impact direct sur la personne concernée, par exemple, pour ce qui regarde l'octroi ou non d'un crédit » ? (62) De surcroît, la loi vise à protéger les intérêts des personnes concernées, ce qui implique qu'en cas de doute, elle doit être interprétée en faveur des droits et de libertés de ces personnes (63).

2.4.4. Mesures organisationnelles et de sécurité

30. — Les banques de données gérées par les compagnies d'assurances (et les courtiers) contiennent de nombreuses informations, dont certaines de nature très sensible. Ces informations à caractère confidentiel sont utilisées au sein de la compagnie par un grand nombre de personnes, ce qui implique que des mesures organisationnelles et techniques doivent être prises afin de garantir la confidentialité (64). Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels (65).

Il faut toujours s'assurer que les données traitées soient exactes et complètes.

Ensuite, seuls les employeurs qui auront besoin de certaines catégories d'informations pour l'exercice de leurs fonctions

(62) Exposé des motifs, p. 52.

(63) Le projet de recommandation du conseil d'Europe sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance, précise à cet égard qu'une exception sur l'interdiction principale de décisions automatisées est légitime « si elles satisfont à une demande introduite par les personnes concernées en vue de la conclusion ou de l'exécution d'un contrat d'assurance ou si les personnes concernées sont admises à faire valoir leur point de vue afin de garantir la sauvegarde de leurs intérêts légitimes » (point 9).

(64) Voy. article 16, § 4 de la LVP.

(65) Voy. article 16, § 4 de la LVP.

pourront avoir accès à ces informations (66). Les personnes travaillant sous l'autorité du responsable du traitement doivent également être informées des dispositions de la législation relative à la protection de la vie privée.

De plus, le traitement ou la gérance de la base de données même peut être réalisée par une personne autre que le responsable du traitement, à savoir un sous-traitant. Ce dernier doit fournir des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements. Il faut encore veiller à ce que ces mesures soient respectées notamment par la stipulation de mentions du traitement, en fixant dans le contrat la responsabilité du sous-traitant, en convenant que ce dernier n'agira que sur la seule instruction du responsable. Ces éléments doivent être consignés par écrit ou sur support électronique (67).

Toute cette liste d'obligations peuvent faire partie intégrante d'une « politique de privacy » de l'entreprise (68).

2.4.5. Notification

31. — Préalablement à la mise en œuvre d'un traitement ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées, le responsable du traitement doit faire une déclaration auprès de la Commission de la protection de la vie privée (69).

Des exemptions peuvent toutefois être prévues par arrêté royal. Cet arrêté royal n'a pas encore été pris mais il semble que le Roi s'est inspiré de la liste figurant dans l'A.R. n° 13 du 12 mars 1996 *portant exemption conditionnelle de l'obligation de déclaration pour certaines catégories de traitements automa-*

(66) On rappelle que les données relatives à la santé doivent en effet être traitées sous la responsabilité d'un professionnel de santé. Une exception est possible avec le consentement écrit de la personne concernée. Le principe de proportionnalité favorise le fait que les personnes qui peuvent accéder à cette catégorie de données seront explicitement tenues par une clause de confidentialité et que des sanctions soient prévues en cas de violation de l'obligation de confidentialité.

(67) Voy. article 16, § 1^{er} de la LVP.

(68) On rappelle que le projet de Recommandation du Conseil de l'Europe sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance contient dans son article 11 une liste de principes plus détaillée qui peut être pratiquée en tant que « check list ».

(69) Pour une critique sur la formulation de cette article, voy. LEONARD, Th. et POULLET, Y., *l.c.*, 392 et s.

tisés de données à caractère personnel qui ne présentent manifestement pas de risque d'atteinte à la vie privée (70).

L'article 6 de cet A.R. stipule que sont exemptés les traitements de données à caractère personnel qui visent exclusivement la gestion de la clientèle ou des fournisseurs du responsable du traitement.

Vu que, dans des fichiers gérés par des compagnies d'assurance, les finalités vont dépasser celles mentionnées ci-avant, une déclaration est obligatoire.

De plus, pour bénéficier de l'exemption, le traitement ne peut se rapporter ni à des données relatives à la santé de l'intéressé, ni à des données sensibles ou judiciaires au sens des articles 6 et 8 LVP. Dans le cadre de l'administration de la clientèle, aucune personne ne peut être enregistrée dans un traitement de données sur la base d'informations fournies par des tiers. Les données ne peuvent être conservées que le temps nécessaire à la gestion normale de l'entreprise du maître du fichier et ne peuvent être communiquées à des tiers, sauf dans le cadre de l'application d'une disposition légale ou réglementaire ou de la gestion normale de l'entreprise.

Il est évident qu'en cas de coassurance, réassurance, expertise, etc. des données sont communiquées à des tiers.

Ensuite, certaines données sensibles sont traitées par la compagnie d'assurance.

On peut en conséquence conclure que dans la majorité des cas, il existe une obligation de notification à la Commission.

3. — TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL POUR DES FINALITÉS EXTERNES

32. — La transmission des informations entre assureurs et au-delà du secteur d'assurance est inhérente au bon fonctionnement des services offerts. Ainsi, des informations seront communiquées en cas de coassurance ou de réassurance. Elles

(70) Voy. projet d'Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, <http://just.fgov.be/html-dgl/tekst.htm>.

seront encore communiquées aux experts investis de la mission d'évaluer les risques et les sinistres, aux organismes publics (sécurité sociale, fonds de garantie), etc (71). Avec le développement des nouvelles technologies, il est non seulement possible de mieux gérer les informations et d'optimiser la communication en vue d'augmenter la qualité des services, mais surtout de rentabiliser l'entreprise en estimant plus efficacement le risque qu'un client représente. Dans ce contexte, on constate — généralement au sein des organismes professionnels — la constitution de mutuelles d'informations permettant de mieux individualiser le client en fonction de sa crédibilité et d'autres paramètres économiques ou sociaux. On examinera dans un premier temps la légitimité de telles initiatives, particulièrement dans le secteur d'assurances, et dans un second temps les normes à respecter.

3.1. — *Le phénomène des mutuelles dans le secteur d'assurance*

33. — Les acteurs économiques offrent leurs services et leurs produits à des prix toujours plus attractifs en raison des lois du marché en minimisant les coûts. Dans ce but, ils exploitent au mieux les informations relatives à leurs potentiels clients. Il est toutefois compréhensible que de telles informations peuvent être utilisées et échangées afin de s'assurer contre certaines risques de « fraude » ou « mauvais payeurs ».

On peut faire une comparaison avec les initiatives de la gestion de risque dans le secteur du crédit à la consommation qui comprennent entre autres l'établissement de fichiers externes par des centrales de crédit. Il s'agit plus particulièrement en Belgique de la mutuelle d'information sur le risque tenu par l'Union Professionnelle du Crédit (U.P.C.) et le fichier établi par la Banque nationale de Belgique. Ces centrales « assurent la centralisation de données relatives aux difficultés de paiement du débiteur défaillant, preneur de crédit, et la communication de ces informations à tout ou partie des professionnels du crédit, participant au système » (72).

(71) Voy. POULLET, Y., « Fichiers d'assurances et respect des libertés », *l.c.*, p. 596.

(72) Voy. LÉONARD, Th., « Fichiers crédits et vie privée : le contexte légal et jurisprudentiel » dans *Les fichiers du crédit*, 1995, p. 6.

Ces deux centrales n'ont toutefois pas la même finalité. La banque de données gérée par la B.N.B. dépend de l'Etat dans le cadre de la lutte contre le surendettement (finalité de protection du consommateur), celle gérée par l'U.P.C. cherche plutôt à minimiser les risques des organismes participants (finalité économique).

Des initiatives similaires existent dans le secteur des assurances. En Belgique il y a depuis 1996 le fichier RSR (Risque Spéciaux/Special Risico's) et géré par le GIE Datassur. Ce fichier englobe une partie importante du secteur de l'assurance I.A.R.D. Cinquante-neuf compagnies y ont adhéré, ce qui représente 88,7 % de l'encaissement dans les branches I.A.R.D (73). En France, il existe le fichier de l'Association pour la Gestion des Informations sur le Risque Automobile (A.G.I.R.A.) qui a pour but l'échange d'informations entre compagnies d'assurance en vue de personnaliser les primes et, accessoirement, de lutter contre la fraude. Pour les assurances-vie, il existe également un fichier des « risques aggravés » au sein de la Caisse Nationale de Prévoyance (C.N.P.). Des initiatives similaires ont également été prises en Angleterre (Association of British Insurers — secteur automobile) et aux Pays-Bas (FISH databank — Fraude en Informatie Systeem Holland).

Pour rappel, ces bases de données ont pour but de distinguer les fraudeurs des non-fraudeurs, de sélectionner les mauvais payeurs et de mieux évaluer les risques dans le but de diminuer le montant des primes (74). Fichée sur une « liste noire » privée, la personne concernée rencontrera donc plus de difficultés pour conclure un contrat ou devra conclure à un tarif plus élevé (75).

34. — Bien que la réduction du risque économique pour les assureurs soit bien légitime et inhérente à la bonne administration de l'entreprise, une telle initiative engendre des risques

(73) Avis n° 21/2000 du 28 juin 2000 de la Commission de la Protection de la vie Privée (Avis d'initiative relatif au fichier RSR (fichier ayant pour but le signalement, entre compagnies d'assurance, des risques spéciaux en assurance incendie, accidents et risques divers) géré par le Groupement d'intérêt économique « Datassur ».

(74) Voy. par exemple article 2 de la convention Datassur.

(75) Voy. Rommelse, A.F., « Zwarte lijsten belangen en effecten van waarschuwingssystemen », 1995, <http://www.registratiekamer.nl/bijltop1-5-35-7.html>.

pour la garantie des libertés fondamentales. Les critères de fichage sont dictés par l'intérêt financier qui est souvent contraire aux intérêts de la personne concernée.

La menace de la vie privée et les autres libertés — la liberté de contracter, de se déplacer en voiture, à la santé etc. — est davantage présente lorsque le traitement de données est réalisé à un *niveau sectoriel* (dans le cas d'espèce, le traitement dépasse les relations client-compagnie d'assurance). Il est ici particulièrement primordial que les conditions et les critères de traitement, étant pour la plupart développés unilatéralement par le secteur, n'entraînent pas une restriction disproportionnée des libertés fondamentales du citoyen.

Ce risque apparaît d'autant plus important dans le contexte d'internationalisation du marché.

Dans le secteur des assurances, et ce contrairement à celui du crédit à la consommation (76), il n'existe aucun cadre légal explicite quant au traitement des données à caractère personnel. Néanmoins, les principes posés par la LVP devront s'appliquer.

On analysera à quelles conditions ces fichiers sont légaux en droit belge, et on examinera la nécessité éventuelle d'une réglementation spécifique dans ce secteur à la lumière de l'article 8 C.E.D.H..

3.2. — Quant à la légitimité et à la proportionnalité du traitement

a) Intérêts, libertés et le principe de proportionnalité

35. — La vie privée ne peut être adéquatement conceptualisée dans le discours juridique qu'en termes de « droit de l'autodétermination » ou de « liberté ». L'idée de l'autonomie de l'individu, valeur centrale dans une société démocratique, se réfère à « l'espace » que l'individu revendique afin de déve-

lopper et de maintenir son identité. La liberté de la vie privée a pour objet « la personne humaine dans sa singularité » et protège « le sujet contre l'expropriation d'un bien de la personnalité par l'Etat et contre l'appropriation d'un tel bien par un autre citoyen » (77). Cette théorie était déjà prônée en 1983 par le Tribunal fédéral allemand en 1983 qui considérait le « droit à l'autodétermination en matière d'information (*Informationelle Selbstbestimmungsrecht*) » comme partie intégrante des droits généraux de la personne humaine (78). Ainsi l'individu dispose du droit de « maîtriser l'image qu'il donne de lui-même dans la société qui doit être protégée des risques d'abus résultant des possibilités actuelles et futures de traitements automatisés de l'information ».

36. — Aucune liberté ou aucun droit subjectif n'ayant un caractère absolu (79), une pondération des intérêts en cause s'impose à la lumière du principe de proportionnalité. Ceci implique selon la doctrine un triple examen (80) : 1) vérifier si les moyens mis en œuvre présentent un lien de causalité suffisant avec l'objectif poursuivi, 2) vérifier si les mesures de traitement envisagées sont indispensables, en s'assurant qu'elles ne peuvent être remplacées par d'autres mesures permettant d'atteindre aussi efficacement le même objectif tout en respectant la liberté éternelle, 3) vérifier que l'atteinte aux libertés ne soit pas disproportionnée par rapport au but poursuivi (81).

En conséquence, les intérêts économiques des assureurs doivent être mis en balance avec la vie privée et les conséquences sur d'autres libertés des personnes concernées.

(77) RIGAUX, F., La vie privée une liberté parmi les autres!, *op. cit.*, pp. 9 et 137.

(78) BverfG., *EUGRZ*, 1983, 588.

(79) « L'individu n'exerce pas une souveraineté absolue sur les faits le concernant; sa personnalité se développant au sein d'une communauté sociale, il ne peut vivre sans communiquer. L'information, même si elle est nominative, est une représentation de la réalité sociale, qui n'est pas uniquement la propriété de l'individu concerné (...). La loi fondamentale résout la dichotomie individu-société en considérant la personne comme une entité liée et insérée dans la société. C'est pourquoi en principe, l'individu doit accepter des restrictions de son 'droit à l'autodétermination en matière d'information' et ce, en faveur de l'intérêt général prépondérant » (BverfG., *EUGRZ*, 1983).

(80) VAN GERVEN, W., « Principe de proportionnalité, abus de droit et droits fondamentaux », *J.T.*, 1992, pp. 305-309.

(81) LEONARD, Th., THUNIS, X., et POULLET, Y., *Id.*, p. 253.

(76) Chapitre 6 de la loi du 12 juin 1991 sur le crédit à la consommation, l'Arrêté royal du 20 novembre 1992 relatif au traitement des données à caractère personnel en matière de crédit à la consommation et l'Arrêté royal du 20 novembre 1992 relatif à l'enregistrement par la Banque nationale de Belgique des défauts de paiement en matière de crédit à la consommation.

La directive 95/46/CE et la LVP ont adopté une conception de « privacy » en terme de « liberté », le jugement quant à la légitimité d'un traitement étant d'ailleurs conçu en terme de proportionnalité.

Ainsi, l'article 5 LVP, contient 6 situations abstraites dans lesquelles l'équilibre des intérêts en présence est présumé être respecté (82).

37. — Dans le cas d'espèce, le point b semble fournir un fondement légitimant les traitements par une centrale de données. Est-ce que le traitement est nécessaire en vue de l'exécution d'un contrat auquel la personne concernée est partie, ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ?

La réponse à la question ne peut être que partiellement positive pour autant qu'il soit envisageable que des tiers, n'ayant aucun lien contractuel avec l'assureur, puissent être fichés. L'enregistrement des données *des tiers* ne peut donc pas être légitimé par le litt. b.

De plus, l'accomplissement des conditions énumérées dans l'article 5 a) jusqu'au point e) est sans préjudice à un *contrôle concret* permettant de révéler une atteinte inacceptable aux droits et intérêts de l'individu (83). Prétendre l'inverse mènerait à des situations absurdes : la nécessité d'un traitement constitue un fondement *a priori* légitime mais ne justifie pas que le traitement soit inconditionnellement légitime ou que

(82) Art. 5. « Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants :

- a) lorsque la personne concernée a indubitablement donné son consentement ;
- b) lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- c) lorsqu'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance ;
- d) lorsqu'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ;
- e) lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;

f) lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi ».

(83) « Le fait de remplir une des conditions de l'article 5 n'implique pas que l'exigence de légitimité de l'article 4, 2°, soit *ipso facto* rencontrée. Les différentes dispositions doivent au contraire s'appliquer cumulativement. » Exposé des motifs, p. 31.

certaines opérations impliquent une violation des libertés fondamentales des personnes concernées.

Ensuite, l'évaluation de la légitimité de la finalité et des opérations effectuées se fait par rapport au principe de proportionnalité (article 4 LVP).

La question principale en cas de mutuelles d'informations dans le secteur des assurances se pose donc comme suit : les risques d'atteinte aux libertés que les personnes concernées encourent ne sont-ils pas disproportionnés par rapport aux intérêts des assureurs ? La réponse à cette question n'apparaît pas immédiatement mais résulte d'un exercice continu de pondération.

Le traitement des données réalisé par les mutuelles d'informations n'est pas toujours évident. On s'attarde aux problèmes les plus épineux et qui doivent rentrer en compte dans l'évaluation de la légitimité du traitement.

b) *Quelques réflexions quant aux risques créés par une mutuelle d'informations*

38. — b.1. Pour rappel, une centrale d'informations gérée par le secteur privé, s'inscrit dans une logique d'ordre économique. Le secteur privé cherche, en facilitant la sélection de ses clients potentiels qui constituent un « bon risque » et en rejetant ainsi ceux qui constituent un « mauvais risque », à améliorer la balance « coûts/bénéfices ».

Le fait que le candidat preneur (ou assuré) soit ou non coupable d'un sinistre ne rentre pas en ligne de compte dans l'évaluation du risque économique. Le simple fait d'être mêlé, de près ou de loin, à un sinistre sera déterminant pour l'assureur lorsqu'il devra décider sous quelles conditions le contrat sera conclu. Ainsi, la notion de culpabilité dans le cadre d'un sinistre n'entre pas en ligne de compte dans la conclusion du contrat. La rationalité économique ne se laisse pas conceptualiser en termes de justice (commettre ou non une faute) (84).

(84) En termes Luhmaniens, il s'agit de deux systèmes (système économique et juridique) où la communication d'un système par rapport à l'autre constitue un « bruit de fond ».

Le fait d'être fiché sur une liste noire sans être coupable ne va pas seulement à l'encontre du « sentiment de justice » mais paraît également disproportionné. Le fichage devient encore plus critiquable lorsque les personnes concernées sont obligées de contracter une assurance (p.ex. RC automobile, clauses contractuelles de bail) en vertu de certaines dispositions légales ou contractuelles (85). Non seulement on est enregistré, mais en plus notre liberté de contracter est fortement réduite : la liberté de se déplacer en voiture (ce qui peut dans certaines cas impliquer une restriction de la liberté de travail), etc.

Les représentants du secteur du crédit défendent la légitimité des centrales d'informations en insistant sur le fait que l'enregistrement ne se fait pas automatiquement, et qu'il n'a qu'une fonction de « clignotant ». Les informations de nature purement « objective », ne forment qu'une indication, une aide dans le processus de décision (86). En réalité, tout dépendra du bon vouloir de l'assureur, la personne concernée se trouvant dans une position de minorité (87).

Lorsque l'A.G.I.R.A. a, dans un premier temps, voulu étendre l'enregistrement à tous les sinistres, que ceux-ci impliquent ou non la responsabilité des intéressés, la CNIL (88) a jugé qu'un tel fichage était excessif au regard des finalités déclarées : l'enregistrement a été jugé excéder les besoins d'information à la personnalisation des primes (89).

En conclusion, il n'est pas certain qu'un fichage du risque indépendant de la responsabilité soit indispensable à la personnalisation des primes et qu'il est donc disproportionné par rapport au but poursuivi. En outre, on dispose déjà de la technique de segmentation du marché, et du système bonus-malus permettant d'individualiser les primes à un certain niveau.

(85) Avis n° 21/2000 du 28 juin 2000, Commission de la protection de la vie privée.

(86) FELIX, F., « Un fichier privé : la mutuelle d'informations sur le risque, présentation, mission et fonctionnement », *Les fichiers du crédit*, Charleroi, L'Observatoire du Crédit et de l'Endettement, 1995, 51, point 3.4, mentionné dans LEONARD, Th., « Centrales de crédit et protection de la vie privée : incertitude et insécurité juridique », *l.c.*, 81.

(87) En fait, l'expérience nous apprend que dans la réalité, le fichage dans le secteur du crédit mène très vite à l'exclusion à contracter.

(88) Commission Nationale de l'Information et des Libertés (soit l'équivalent français de notre Commission Vie Privée Française).

(89) WILLIAMS, S., note d'étude de la CPVP.

39. — b.2. Un autre problème qui se pose souvent dans le contexte d'un fichage sur une « liste noire », est de déterminer à partir de quel moment un consommateur « risqué » peut légitimement être fiché. On est familiarisé avec ce contentieux concernant ce problème dans le contexte du crédit à la consommation (90). En l'absence d'une législation spécifique déterminant les conditions d'un enregistrement, la légitimité doit de nouveau être évaluée par rapport au principe de proportionnalité.

Il n'est pas sans importance d'indiquer qu'en faisant la pondération d'intérêts, on prendrait en compte le fait qu'il existe un rapport de force « asymétrique » entre une compagnie d'assurance et le client. D'ailleurs, s'il y a un désaccord entre les parties par exemple concernant l'existence d'une obligation de paiement, l'assureur peut toujours « menacer » de fichier l'adversaire. Hormis l'hypothèse où le reproche de non-prestation n'est pas fondé, on pense plus particulièrement au cas où un preneur d'assurances s'appuie à juste titre sur l'*exceptio non adimpleti contractus*. Le fait que l'*exceptio* soit interprétée comme un « défaut de paiement » par l'entreprise évoquant l'enregistrement, nous paraît injuste.

De plus, bien que la liberté de commerce n'empêche pas qu'un seul acteur de marché puisse décider de ne pas vouloir contracter avec un individu, il faut néanmoins distinguer la situation où l'entière d'un secteur exclut ce même individu pour ne pas avoir payé ses dettes (91).

Le défaut de paiement doit donc avoir une certaine gravité et être de nature structurelle. Les finalités de la banque de données ne peuvent pas être perverses en essayant que l'enregistrement rende les obligations des clients « plus effectives » (92).

(90) Civ. Liège, 11 mars 1987, *J.L.M.B.*, 1987, pp. 549 et s.; Civ. Liège, 2 décembre 1987, *J.L.M.B.*, 1988, pp. 122 et s.; Cour d'appel Liège, 3^e Ch., 6 juin 1991, *D.I.T.*, 1994, pp. 32 et s.; Tribunal de Première instance (prés.), Brux., 13 septembre 1995, *D.C.C.R.*, pp. 57 et s.

(91) Sauf dans l'hypothèse où il s'agit d'un intérêt très grand (voy. ROMMELSE, A.F., *l.c.*, Registratiekamer, mei 1995, p. 14).

(92) *Ibidem.*, pp. 14-15 : « Indien bij kleine onbetaalde vorderingen iemand al op een zwarte lijst wordt geplaatst, is het doel van een dergelijke lijst niet het weren van oplichter e.d. In die gevallen vormt een zwarte lijst in wezen een sterke prikkel om aan de betalingsverplichting te voldoen. Zolang de debiteur niet betaalt, wordt voor hem immers in meer of mindere mate de weg afgesneden naar de betreffende voorziening » en « Het doel oplichters e.d. te

En tout cas, des garde-fous procéduraux peuvent être recommandés afin de compenser ces problèmes. Il est vrai, l'article 15 LVP stipule que la personne concernée a le droit d'exiger qu'une information contestée soit mentionnée. Cependant le fichage a à ce moment déjà été réalisé. Ne témoignerait-il pas plus d'un respect de la proportionnalité des intérêts en cause, le fait de prévoir que l'assuré ou le tiers qui fait l'objet d'un fichage éventuel soit informé et dispose de la possibilité de s'adresser vers un organe indépendant ?

40. — b.3. Le même raisonnement concernant le respect du principe de proportionnalité vaut pour les cas de « fraude » (93). On peut distinguer les différentes sortes de fraude avec une sévérité divergente. Le risque est cependant imminent que toutes ces catégories, pour autant qu'une diversification entre celles soit faite, soient généralisées comme des cas de fraude « tout court ».

De surcroît, si une personne est fichée pour des *présomptions* de fraude, le risque est réel qu'elle puisse être qualifiée de « fraudeuse » tout simplement, les informations qui ont en principe une fonction de « clignotant » étant considérées comme véridiques (94). Par exemple, le fait que la déclaration ne corresponde pas à des enregistrements antérieurs, n'implique pas que la personne concernée est de mauvaise foi. On se demande dès lors si les contraintes économiques ne mineront pas la notion de fraude de son contenu juridique en l'utilisant comme prétexte facile pour justifier le fichage.

Indiquons également que la décision légitimant l'enregistrement est prise par les participants au système de mutuelle. L'individu est donc enregistré en l'absence d'une décision officielle, en l'absence d'une procédure où ses droits de défense

ueren is een belang van de bedrijfstak. Het doel dat elke vordering op tijd wordt voldaan is geen bedrijfstakbelang, maar uitsluitend een eigenbelang ».

(93) Il y a beaucoup d'incertitude quant à la définition de fraude. Le Petit Robert pose la définition suivante : « Action faite de mauvaise foi dans le but de tromper ».

(94) Dans le cadre du fichier R.S.R. on pense plus particulièrement au fichage sous code 16 (refus d'intervention de la part de l'assureur à la suite de manquements à la souscription, mesures de prévention exigées par l'assureur mais non réalisées par l'intéressé, comportement inconscient) et 31 et 32, à savoir les données relatives aux « risques refusés » lorsque la déclaration du candidat à l'assurance concernant le risque à assurer 1) ne correspond pas avec les enregistrements antérieurs dans le RSR; 2) ne correspond pas avec la réalité.

sont garantis (comme c'est le cas concernant le casier judiciaire). La CPVP a dès lors décidé qu'elle « estime que le traitement de [données qui font état des suspicions] a un caractère plus dommageable et plus délicat encore, dans la mesure où elles n'ont pas été soumises à l'examen du juge ni à une quelconque procédure contradictoire » (95).

41. — b.4. De plus, il est possible que des informations judiciaires fassent l'objet d'une banque de données gérée par une mutuelle (pensons par exemple au recours exercé par l'assureur, à la reconnaissance judiciaire de responsabilité, etc).

On a déjà souligné qu'il est peu probable que l'exemption prévue par l'article 8, § 2 b) (traitement nécessaire à la réalisation de finalités par ou en vertu d'une loi) puisse être applicable aux compagnies d'assurances et que de plus, elle nous paraisse devoir être exclue pour une mutuelle d'informations vu que l'obligation d'évaluation de risque n'incombe pas à cette dernière (96).

Dans le cas du fichier RSR géré par la GIE Datassur, les « faits objectifs » ne sont pas repris, mais bien les mentions et les codes indicatifs déduits de tels faits (97). Cette pratique semble positive pour autant que les faits objectifs ne puissent pas être connus par le participant accédant au fichier. Toutefois, l'utilisation de codes en vue de garantir un minimum de respect pour la vie privée et les libertés, semble être ambigu. La réalité complexe ne peut être perçue dans une liste de catégories prédéfinies. Le problème ne se situe pas directement

(95) Avis n° 21/2000 du 28 juin 2000.

(96) La CPVP a décidé quant au fichier RSR géré par GIE Datassur qu'« en vertu de l'article 8 de la loi, le traitement de ce type de données n'est légal que s'il effectue soit sous le contrôle d'une autorité publique ou d'un officier ministériel au sens du Code judiciaire, lorsque ce traitement est nécessaire à l'exercice de leurs tâches, soit par d'autres personnes de droit public ou de droit privé pour autant que la gestion de leur propre contentieux l'exige. Le consentement de l'intéressé ne suffit pas à lever l'interdiction », Avis n° 21/2000 du 28 juin 2000.

(97) Il existe une incertitude quant à la qualité des « codes ». Bien qu'il soit incontestable qu'il s'agisse de données personnelles, il n'est pas sûr qu'ils puissent être qualifiés de « données judiciaires ». L'exposé des motifs distingue entre « données relatives à une information sensible » et « données révélant une information sensible » (Exposé des motifs, p. 33-34). Dans son Avis n° 21/2000, la CPVP ne semble pas combler cette problématique. A première vue, elle semble accepter que les informations traitées par Datassur constituent de telles données, mais considère que les codes se référant aux suspicions que « ces données ne sont pas des données judiciaires au sens de l'article 8 de la loi ». Il aurait été préférable que la CPVP prenne un point de vue clair en la matière.

dans le fait que la réalité des faits soit présentée de façon réduite, mais que cette réduction soit considérée comme réelle. Bien que les informations n'aient qu'une fonction indicative, le risque existe qu'ils soient généralisés, et ce en dénegation de facettes plus nuancées de la réalité.

c) *La légitimité pondérée*

42. — La légitimité d'un traitement conceptualisée comme un équilibre entre les intérêts et libertés en cause, ne se laisse pas percevoir en termes absolus. Ce jugement reflète en fait les valeurs qu'une société ou une communauté estime précieuses, et est *juridicisé*, comme mentionné ci-dessus, en termes de pondération d'intérêts par rapport au principe de proportionnalité (*supra* n° 35 e.s.).

La légitimité d'une centrale de données dans le secteur d'assurance est pour sa plus grande partie enracinée dans l'article 5 LAT. Il est hors discussion qu'un assureur doit disposer des moyens adéquats à l'évaluation du risque dans les circonstances qui se présentent dans un cas concret. Toutefois, la mise sur pied d'une banque de données sectorielle dépasse le domaine des relations contractuelles et peut difficilement trouver sa *seule légitimation* dans cet article. L'article 5 LAT est certes une disposition pertinente qui plaide pour la légitimité d'une telle entreprise qui doit sans doute être prise en compte dans notre jugement, mais elle ne nous paraît pas être une condition suffisante.

La raison est évidente. *La constitution d'une centrale d'informations ne place plus la personne concernée devant un acteur du marché, mais face à tout un secteur du marché. Un glissement s'opère du niveau individuel vers un niveau sectoriel. Les conséquences éventuelles pour les libertés individuelles seront donc d'ordre plus sévère.*

Ainsi, les critères de fichage et les conditions se basent sur l'intérêt du secteur, plutôt que sur l'intérêt de l'individu. Il est vrai qu'une diminution des prix des primes sert l'intérêt du preneur d'assurances, mais elle fait aussi en grande partie abstraction d'autres intérêts qui ne sont pas estimables en termes pécuniaires.

Ces critères forment une sorte de « quasi-législation » qui est unilatéralement imposée par un secteur, et inspirée par les intérêts de celui-ci. Bien que l'on ne soit pas en soi opposé à l'autorégulation, on est d'avis que les droits fondamentaux du citoyen en pourraient être bafoués.

La question de la légitimité peut être reformulée, quitte à être provocante, en termes de *justesse* : « Est-ce qu'une obligation légale dans le chef de la personne concernée à l'encontre de l'assureur justifie en soi que tout un secteur puisse restreindre l'autonomie de la première » ? Quel est en fait la différence avec une peine ? Quelles sont les garanties démocratiques ?

Il ne serait pas opportun de donner un verdict *in abstracto*, le principe de proportionnalité devant être appliqué dans les circonstances concrètes.

Toutefois, on a démontré sous le point b. que l'atteinte aux libertés est, le cas échéant, souvent réelle. Ce risque se fait davantage sentir lorsque les nouveaux médias permettent facilement d'atteindre ces bases de données. On peut s'imaginer que dans le contexte de la globalisation des marchés, ces bases de données seront *fusionnées*. De tels projets se trouvent déjà dans le monde du crédit (98).

Enfin, on est d'avis qu'en créant une situation menaçante pour les libertés des individus, il faut faire pencher la balance en faveur de celles-ci. Il s'agit notamment des limitations aux droits qui sont considérés fondamentaux dans notre société et qui sont protégés par la Constitution et les textes internationaux (Convention n° 108 Conseil d'Europe, article 8 C.E.D.H.) (99).

(98) « Europese uitwisseling van ondernemingskredieten in de maak — België wisselt kredietgegevens uit met Duitsland », *Financieel Economische Tijd*, 27 juin 2000.

(99) Voy. GUTWIRTH, S., « De toepassing van het finaliteitsbeginsel van de privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens », dans *T.P.R.*, 1993, pp. 1409-1477; voy. également DE HERT, P., Artikel 8 E.V.R.M. en het Belgisch recht — De bescherming van privacy, gezin, woonst en communicatie, Mys & Breesch, Gent, 1998.

3.3. — La légalité du traitement : quelques brèves remarques quant à certains droits subjectifs

43. — La légitimité d'un traitement n'emporte pas en soi la légalité. Celle-ci dépendra du respect des autres principes et droits subjectifs inscrits dans la LVP. Rappelons que la personne doit être adéquatement informée quant au traitement des données la concernant, qu'elle dispose d'un droit d'accès et de rectification, que la prise des décisions sur la base d'un traitement automatisé est interdite, que la sécurité des données doit être garantie et qu'une notification auprès la CPVP est obligatoire. On se réfère quant à ce point à la première partie de cette contribution (cf. *supra* n° 2.4), mais en citant encore trois remarques qui sont d'importance dans le contexte d'une mutuelle d'informations.

44. — D'abord l'information préalable devra être complète et transparente, afin de garantir la loyauté du traitement (article 9 LVP). Ceci signifie que la personne concernée (preneur d'assurances/assuré/tiers) sera informée de l'existence du fichier et de ses finalités et du fait que les informations puissent être communiquées aux assureurs-participants. La CPVP ajoute encore que « dans l'hypothèse où l'information du candidat se fait sous la forme d'une mention dans les conditions générales de la police d'assurance, la personne concernée n'a, en pratique, que rarement l'occasion de prendre connaissance des conditions générales avant de signer un contrat et que de ce fait elle n'est pas suffisamment informée. Cette information devrait être communiquée de manière claire à la personne concernée, par exemple, au bas de la proposition d'assurance, à proximité de l'emplacement prévu pour la signature et en lettres lisibles » (100).

L'enregistrement se passera au moment de la conclusion d'un contrat ou en cas de sinistre. L'obligation d'information peut au moyen d'une convention être déléguée aux membres de la mutuelle.

45. — Ensuite, des initiatives de centralisation de données, créent une demande des informations. Il n'est dès lors pas

(100) Avis n° 21/2000 du 28 juin 2000.

impossible que le droit d'accès soit souvent détourné de sa finalité. Plus spécifiquement, il faut éviter que les acteurs sociaux qui se retrouvent dans une position majoritaire ne contraignent pas la personne concernée à exercer son droit d'accès, et ce dans le but d'obtenir un surplus d'informations.

Il est toutefois difficile d'éviter de telles tendances (qui sont inhérentes aux lois du marché) et qui augmenteront avec la croissance du nombre de banques de données.

46. — Finalement, les risques qui sont créés par une centrale de données peuvent dans certains cas être contrebalancés par l'attribution d'un droit d'opposition (système de « opt-out »).

Il est notamment prévu par l'article 12 LVP que toute personne a le droit de s'opposer à ce que des données la concernant soient traitées, pour autant qu'elle fasse état de raisons sérieuses et légitimes tenant à une situation particulière.

Une situation particulière pourrait survenir lorsqu'un défaut de paiement minime ou sans caractère structurel, ou qu'une succession de sinistres n'emporte pas la responsabilité de l'intéressé (101).

4. — CONCLUSION

47. — Les services et produits que les assureurs offrent nécessitent une grande quantité d'informations. La LAT contient à ce sujet quelques dispositions qui légitiment la collecte et l'enregistrement des données relatives aux preneurs d'assurances et aux assurés. Cependant, la légalité de ces traitements doit également respecter les dispositions de la LVP. Le traitement doit ainsi être entouré des garanties de transparence et de sécurité, ce qui ne peut selon nous que renforcer la confiance du client.

Cependant, le traitement de données « sensibles » ne sera pas évident, et il apparaît dès lors que le législateur n'a pas, lors de la transposition de la Directive 95/46/CE, assez anticipé les

(101) Avis n° 21/2000 du 28 juin 2000.

problèmes qui pouvaient naître dans ce contexte des assurances.

Les informations ne seront pas seulement être utilisées à des finalités purement internes, mais vont bien évidemment circuler dans — et parfois hors de — ce secteur spécifique. On s'est dans ce *cadre* focalisé sur le phénomène de mutuelles d'informations privées, et on s'est surtout interrogé sur la question de la légitimité d'un tel traitement.

La conclusion qui ne peut se traduire qu'en termes de proportionnalité, dépendra surtout de la situation concrète. Néanmoins, la réalisation d'une centrale de données est le résultat d'une initiative sectorielle, ce qui constitue en réalité une sorte de « quasi-législation ». Le test de la légitimité doit en conséquence prendre en compte le contexte concret, et plus particulièrement la restriction potentielle des libertés de la personne concernée.

On pourrait considérer que d'un point de vue strictement juridique, une législation spécifique soit superflue. D'ailleurs, toutes les garanties se trouvent déjà inscrites dans la LVP et les conditions de traitement sont légitimes pour autant que la balance d'intérêts en cause soit respectée. Toutefois, dans la réalité, le risque existe que les modalités de traitement soient inspirées par des motifs économiques et reflètent en grande partie les intérêts (légitimes) du secteur. On caricature peut-être mais il est incontestable que le but n'est pas, dans le cas d'espèce, la protection du consommateur, mais consiste en un renforcement des intérêts des assureurs.

Il nous paraît qu'une législation spécifique doive être prise en compte en analogie avec le secteur du crédit à la consommation, qui pourrait alors prendre en compte les correctifs nécessaires afin d'équilibrer les intérêts en cause.

Une telle initiative nous semble surtout défendable d'un point de vue démocratique et suivant la doctrine des obligations positives dans le cadre de l'article 8 C.E.D.H., dans la mesure où les normes existantes n'atteignent pas leur but et dans la mesure où on se voit confronté, dans certains cas, à une discrimination de fait.